

Математическая логика

mk.cs.msu.ru → Лекционные курсы → Математическая логика (318, 319/2, 241, 242)

Блок 52

Спецификация систем
при помощи темпоральных логик

Лектор:

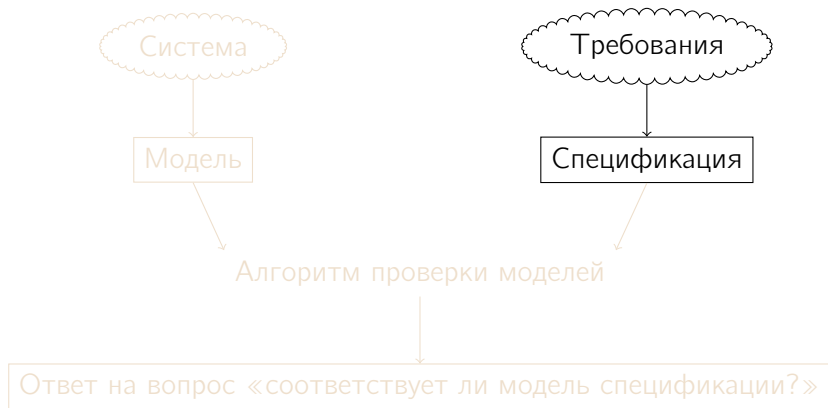
Подымов Владислав Васильевич

E-mail:

valdus@yandex.ru

ВМК МГУ, 2025, февраль–май

Вступление



Вступление

Оказалось, что в качестве основы модели распределённой системы можно выбрать модели Крипке:
интерпретацию формул модальной логики

Тогда естественно возникает вопрос:
а нельзя ли в качестве основы языка спецификаций
выбрать язык модальных формул?

При положительном ответе можно будет использовать
все факты, относящиеся к модальным формулам
и их выполнимости в тех или иных моделях

Вступление

Основные препятствия на пути к использованию модальных формул в качестве спецификаций:

- ▶ **Техническое:** когда язык спецификаций выбран, следует строго, чётко и разумно (*адекватно*) поставить задачу проверки соответствия модели и спецификации
- ▶ **Описательное:** если язык спецификаций оказался слишком невыразительным, то требуется найти достаточно выразительное расширение этого языка
- ▶ **Алгоритмическое:** если эффективная проверка соответствия модели и спецификации оказалась невозможной, то требуется найти достаточно эффективно анализируемое сужение этого языка

CTL*

CTL* — это язык спецификаций, который:

- ▶ Основан на модальной логике
- ▶ Включает в себя LTL и CTL
 - ▶ и, в частности, содержит все те буквы (**G**, **F**, **A** и **E**), из которых в блоке 50 строились модальности $\Box$, $\Diamond$ и другие
- ▶ Позволяет поставить и решить задачу проверки соответствия модели и формулы
 - ▶ То есть задачу проверки выполнимости формулы на СП

CTL*: синтаксис и семантика

Синтаксис формул CTL* над множеством атомарных высказываний AP задаётся БНФ

$$\begin{aligned}\Phi &::= \top \mid p \mid (\Phi \& \Phi) \mid (\Phi \vee \Phi) \mid (\neg \Phi) \mid (\Phi \rightarrow \Phi) \\ &\quad \mid (\mathbf{A}\varphi) \mid (\mathbf{E}\varphi) \\ \varphi &::= \Phi \mid (\varphi \& \varphi) \mid (\varphi \vee \varphi) \mid (\neg \varphi) \mid (\varphi \rightarrow \varphi) \\ &\quad \mid (\mathbf{F}\varphi) \mid (\mathbf{G}\varphi) \mid (\mathbf{X}\varphi) \mid (\varphi \mathbf{U} \varphi),\end{aligned}$$

где

- ▶ Φ — формула CTL*, или, по-другому, формула состояния,
- ▶ φ — формула пути и
- ▶ $p \in AP$

Для двух видов формул соответственно определяется два вида выполнимости:

- ▶ Выполнимость формулы состояния Φ в заданном состоянии s СП M : $M, s \models \Phi$
- ▶ Выполнимость формулы пути φ на заданном бесконечном пути π в СП M : $M, \pi \models \varphi$

CTL*: синтаксис и семантика

Синтаксис формул CTL* над множеством атомарных высказываний AP задаётся БНФ

$$\begin{aligned}\Phi &::= \mathbb{t} \mid p \mid (\Phi \& \Phi) \mid (\Phi \vee \Phi) \mid (\neg \Phi) \mid (\Phi \rightarrow \Phi) \\ &\quad \mid (\mathbf{A}\varphi) \mid (\mathbf{E}\varphi) \\ \varphi &::= \Phi \mid (\varphi \& \varphi) \mid (\varphi \vee \varphi) \mid (\neg \varphi) \mid (\varphi \rightarrow \varphi) \\ &\quad \mid (\mathbf{F}\varphi) \mid (\mathbf{G}\varphi) \mid (\mathbf{X}\varphi) \mid (\varphi \mathbf{U} \varphi),\end{aligned}$$

Приоритеты операций: $\neg$, $\mathbf{A}$, $\mathbf{E}$, $\mathbf{F}$, $\mathbf{G}$ и $\mathbf{X}$; затем $\mathbf{U}$;

затем остальные операции с обычными приоритетами

Символ $\mathbb{t}$, связки $\&$, $\vee$, $\neg$, $\rightarrow$

и атомарное высказывание p имеют «привычный» содержательный смысл

Буквы $\mathbf{A}$ и $\mathbf{E}$ — это **кванторы пути**:

- ▶ « $\mathbf{A}\varphi$ » = «для любого бесконечного пути, исходящего из текущего состояния, верно φ » и
- ▶ « $\mathbf{E}\varphi$ » = «существует бесконечный путь, исходящий из текущего состояния и такой что для него верно φ »

CTL*: синтаксис и семантика

Синтаксис формул CTL* над множеством атомарных высказываний AP задаётся БНФ

$$\begin{aligned}\Phi &::= \top \mid p \mid (\Phi \& \Phi) \mid (\Phi \vee \Phi) \mid (\neg \Phi) \mid (\Phi \rightarrow \Phi) \\ &\quad \mid (\mathbf{A}\varphi) \mid (\mathbf{E}\varphi) \\ \varphi &::= \Phi \mid (\varphi \& \varphi) \mid (\varphi \vee \varphi) \mid (\neg \varphi) \mid (\varphi \rightarrow \varphi) \\ &\quad \mid (\mathbf{F}\varphi) \mid (\mathbf{G}\varphi) \mid (\mathbf{X}\varphi) \mid (\varphi \mathbf{U} \varphi),\end{aligned}$$

Буквы **F**, **G**, **X**, **U** — это темпоральные операторы:

- ▶ «**F** φ » = «когда-нибудь, рано или поздно, станет верно φ »
- ▶ «**G** φ » = «всегда будет верно φ »
- ▶ «**X** φ » = «в следующем состоянии будет верно φ » (neXt step)
- ▶ « $\varphi \mathbf{U} \psi$ » = «когда-нибудь станет верно ψ ,
а пока оно не стало верным, обязательно верно φ » (Until)

CTL*: синтаксис и семантика

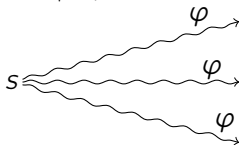
Отношения выполнимости формул для СП $M = (S, S_0, \mapsto, L)$, состояния s и бесконечного пути π заданы следующими правилами:

- ▶ Соотношение $M, s \models \mathbb{t}$ верно всегда
- ▶ $M, s \models p$, где $p \in AP \iff p \in L(s)$
- ▶ $M, s \models \Phi \& \Psi \iff M, s \models \Phi$ и $M, s \models \Psi$
- ▶ $M, \pi \models \varphi \& \psi \iff M, \pi \models \varphi$ и $M, \pi \models \psi$
- ▶ $M, s \models \Phi \vee \Psi \iff M, s \models \Phi$ или $M, s \models \Psi$
- ▶ $M, \pi \models \varphi \vee \psi \iff M, \pi \models \varphi$ или $M, \pi \models \psi$
- ▶ $M, s \models \neg \Phi \iff M, s \not\models \Phi$
- ▶ $M, \pi \models \neg \varphi \iff M, \pi \not\models \varphi$
- ▶ $M, s \models \Phi \rightarrow \Psi \iff M, s \not\models \Phi$ или $M, s \models \Psi$
- ▶ $M, \pi \models \varphi \rightarrow \psi \iff M, \pi \not\models \varphi$ или $M, \pi \models \psi$
- ▶ $M, \pi \models \Phi$ для формулы состояния $\Phi \iff M, \pi[1] \models \Phi$
 - ▶ $\pi[i]$ — i -е состояние пути π при нумерации с единицы

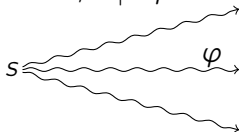
CTL*: синтаксис и семантика

Отношения выполнимости формул для СП $M = (S, S_0, \mapsto, L)$, состояния s и бесконечного пути π заданы следующими правилами:

- ▶ $M, s \models \mathbf{A}\varphi \iff$ для любого бесконечного пути π в M , исходящего из s , верно $M, \pi \models \varphi$



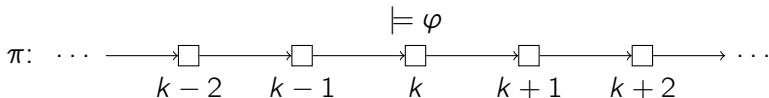
- ▶ $M, s \models \mathbf{E}\varphi \iff$ существует бесконечный путь в M , исходящий из s и такой что $M, \pi \models \varphi$



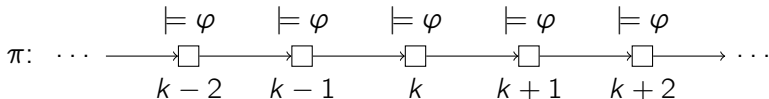
CTL*: синтаксис и семантика

Отношения выполнимости формул для СП $M = (S, S_0, \mapsto, L)$, состояния s и бесконечного пути π заданы следующими правилами:

- ▶ $M, \pi \models \mathbf{F}\varphi \Leftrightarrow$ существует номер k , $k \geq 1$, такой что $M, \pi^k \models \varphi$
- ▶ π^k — суффикс пути π , начинающийся с k -го состояния



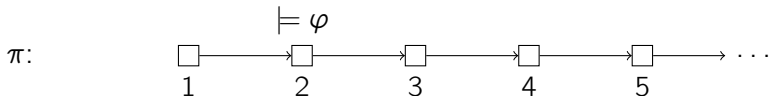
- ▶ $M, \pi \models \mathbf{G}\varphi \Leftrightarrow$ для любого номера k , $k \geq 1$, верно $M, \pi^k \models \varphi$



CTL*: синтаксис и семантика

Отношения выполнимости формул для СП $M = (S, S_0, \mapsto, L)$, состояния s и бесконечного пути π заданы следующими правилами:

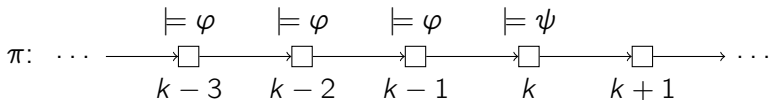
$$\blacktriangleright M, \pi \models \mathbf{X}\varphi \Leftrightarrow M, \pi^2 \models \varphi$$



$$\blacktriangleright M, \pi \models \varphi \mathbf{U} \psi \Leftrightarrow \text{существует номер } k, k \geq 1, \text{ такой что}$$

$$\blacktriangleright M, \pi^k \models \psi \text{ и}$$

$$\blacktriangleright \text{для любого номера } m, \text{ такого что } 1 \leq m < k, \text{ верно } M, \pi^m \models \varphi$$



CTL*: постановка задачи проверки моделей

Формула CTL* φ выполняется на СП M ($M \models \varphi$),
если она выполняется в любом начальном состоянии системы M

Задача проверки моделей для CTL* формулируется так:
для заданной **конечной** системы переходов M
и заданной формулы φ CTL*
проверить справедливость соотношения $M \models \varphi$

CTL* и LTL

Формула LTL — это формула CTL* вида $\mathbf{A}\varphi$,

в которой подформула φ не содержит ни одного квантора пути

По сравнению с блоком 50, в предложенном определении формулы LTL

- ▶ Содержится квантор $\mathbf{A}$:

при использовании формулы LTL в качестве спецификации этот квантор принято включать в формулу, явно или неявно

- ▶ Содержатся темпоральные операторы $\mathbf{X}$ и $\mathbf{U}$:

это примеры модальностей, отличных от $\Box$ и $\Diamond$

Бесконечному пути π СП $M = (S, S_0, \mapsto, L)$ можно сопоставить интерпретацию $\mathcal{I}_\pi = (\mathbb{N}, \leq, \mathcal{L})$ LTL, в которой указаны по порядку все множества атомарных высказываний, помечающие состояния пути:

$$\mathcal{L}(k) = L(\pi[k])$$

Тогда выполнимость формулы LTL φ на пути π СП совпадает с её выполнимостью в интерпретации $\mathcal{I}_\pi$ LTL в том смысле,

как это вводилось в рассказе про модальные логики,

и соотношение $M \models \varphi$ означает, что все вычисления M

обладают свойством правильности, записанным в виде формулы φ

CTL* и LTL

Примеры спецификаций на языке LTL:

- ▶ Данные на печать передаются не более чем одним принтером:

$$\mathbf{AG}\neg(\textit{print}_1 \ \& \ \textit{print}_2)$$

- ▶ После завершения процедур начисления стипендии и зарплаты на счёте будет ровно 1 001 000 рублей:

$$\mathbf{AFG}p_{\text{счёт}=1\ 001\ 000}$$

- ▶ На следующем шаге после оплаты напитка он будет выдаваться:

$$\mathbf{AG}(\neg\textit{paid} \ \& \ \mathbf{X}\textit{paid} \rightarrow \mathbf{XX}(\textit{serve}_t \vee \textit{serve}_c))$$

- ▶ Если компьютер достаточно часто посылает запрос на печать, то рано или поздно он начнёт печатать:

$$\mathbf{A}(\mathbf{GF}\textit{request} \rightarrow \mathbf{F}\textit{print})$$

- ▶ Если идёт печать, то сеанс печати рано или поздно завершится, и до завершения принтер будет занят:

$$\mathbf{AG}(\textit{print} \rightarrow \textit{busy}\mathbf{U}\neg\textit{print})$$

CTL* и CTL

Формула CTL — это формула CTL* частного вида, отвечающего БНФ

$$\begin{aligned}\Phi &::= \texttt{t} \mid p \mid (\Phi \& \Phi) \mid (\Phi \vee \Phi) \mid (\neg \Phi) \mid (\Phi \rightarrow \Phi) \\ &\quad \mid (\mathbf{A}\varphi) \mid (\mathbf{E}\varphi) \\ \varphi &::= (\mathbf{F}\Phi) \mid (\mathbf{G}\Phi) \mid (\mathbf{X}\Phi) \mid (\Phi \mathbf{U} \Phi),\end{aligned}$$

То есть в формуле CTL под квантором пути обязательно располагается темпоральный оператор, и под ним — формула состояния

Иными словами, в формуле CTL кванторы пути и темпоральные операторы используются только в парах:

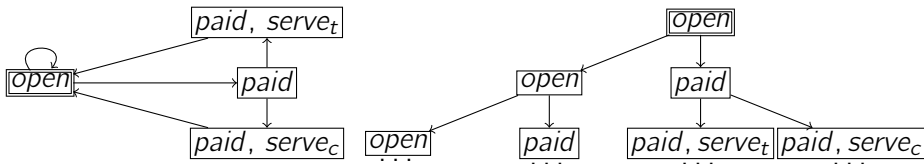
AG, EG, AF, EF, AX, EX, AU, EU

CTL* и CTL

В блоке 50 рассказывалось, что формулы CTL интерпретируются на рефлексивно-транзитивных замыканиях особых бесконечных деревьев. Такое бесконечное дерево можно понимать как **развёртку** системы переходов:

- ▶ Корень — это выбранное начальное состояние
- ▶ Вершина развёртки отвечает конечному пути в СП и размечена теми же атомарными высказываниями, что и последняя вершина пути
- ▶ Дуга $v_1 \rightarrow v_2$ в развёртке означает, что путь v_1 можно продолжить до пути v_2 , добавив один переход

Например, ниже изображены СП и фрагмент её развёртки



CTL* и CTL

Примеры спецификаций на языке CTL для кофейного автомата:

- ▶ В самом начале работы автомата приёмник монет открыт, в нём нет монеты, и автомат ничего не выдаёт:

$$open \ \& \ \neg paid \ \& \ \neg serve_t \ \& \ \neg serve_c$$

- ▶ Нельзя сделать так, чтобы автомат выдал напиток, не имея монеты в приёмнике:

$$\neg \mathbf{EF}(\neg paid \ \& \ (serve_c \vee serve_t))$$

- ▶ Если в приёмнике есть монета, то рано или поздно он выдаст напиток ...

$$\mathbf{AG}(paid \rightarrow \mathbf{AF}(serve_c \vee serve_t))$$

- ▶ ... но этот напиток не обязан быть чаем ...

$$\mathbf{EF}(paid \ \& \ \mathbf{EG}\neg serve_t)$$

- ▶ ... но при желании можно, опустив монету в приёмник, получить чай

$$\mathbf{AG}(\neg paid \rightarrow \mathbf{AX}(paid \rightarrow \mathbf{EF}serve_t))$$